

Fig. 2

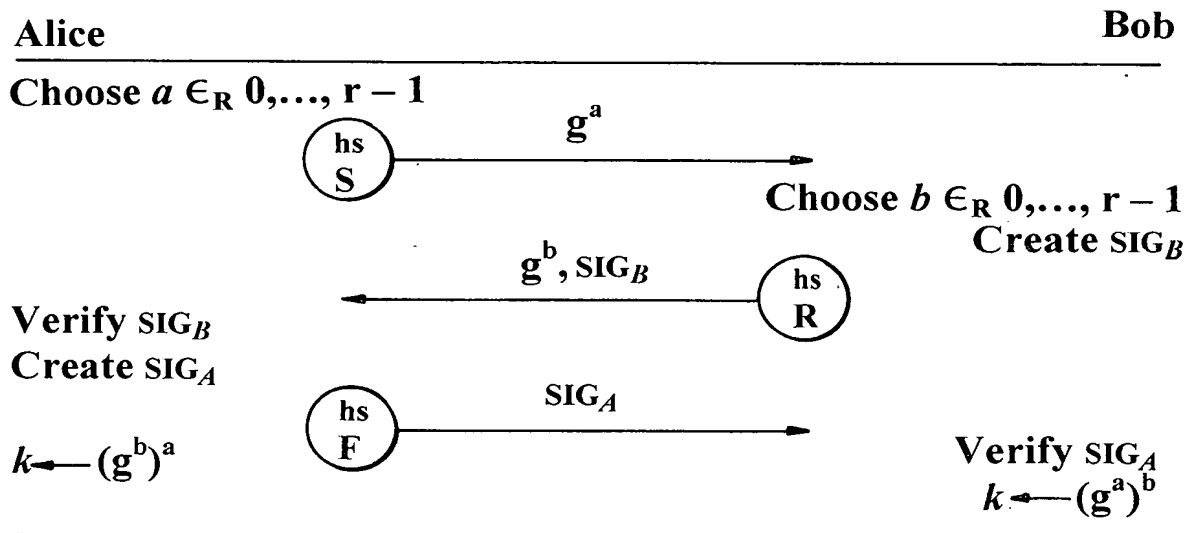


Fig. 3

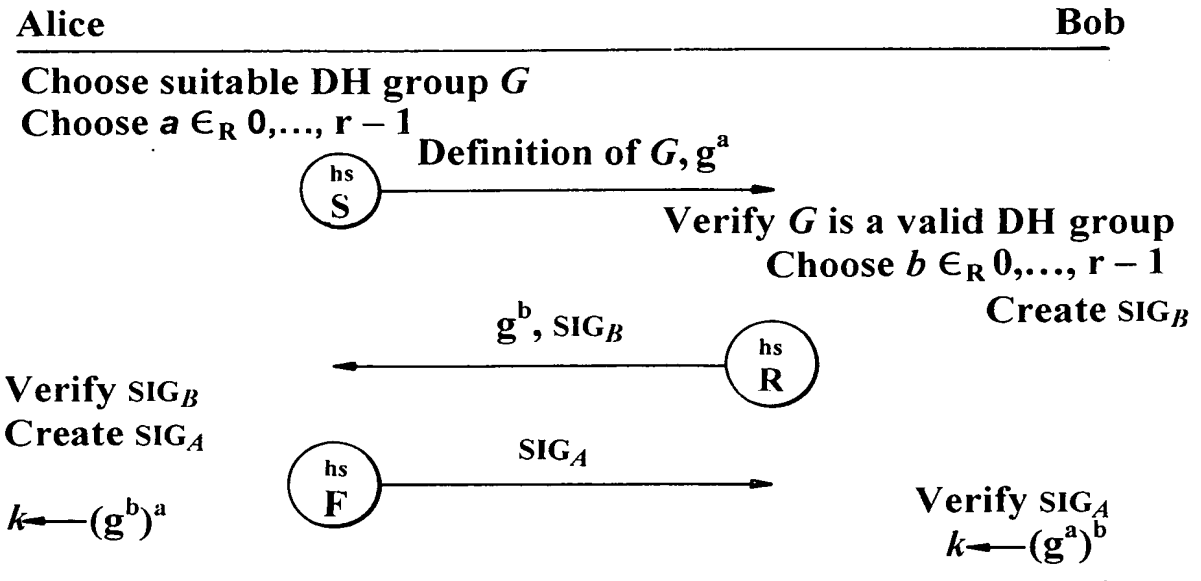


Fig. 4

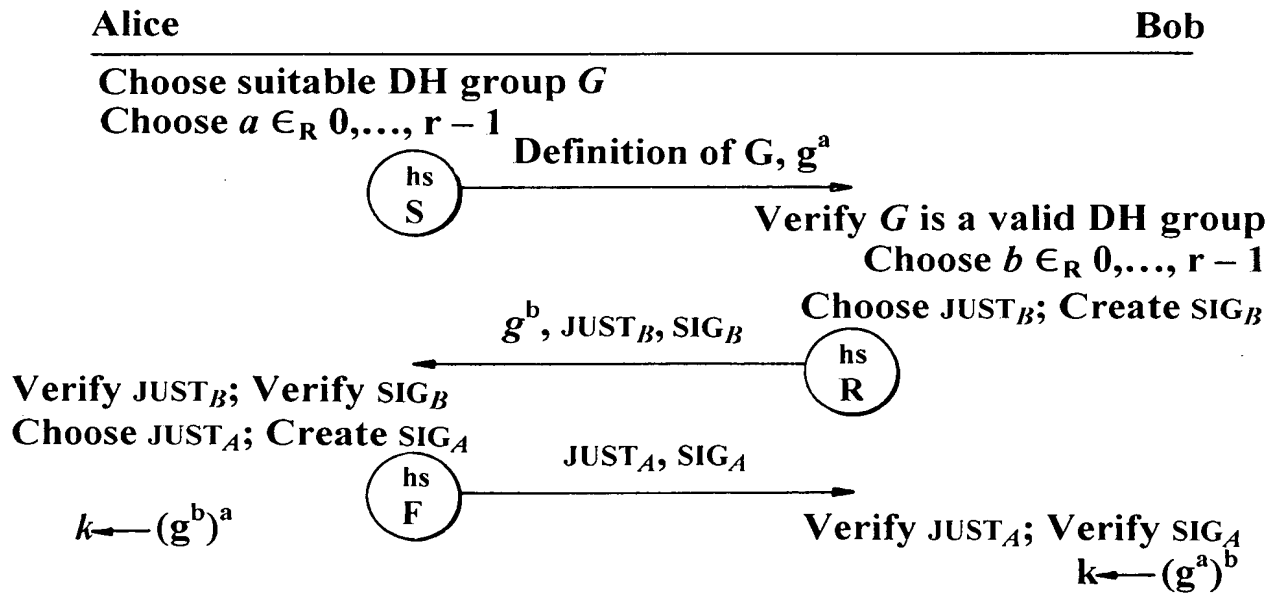


Fig. 5

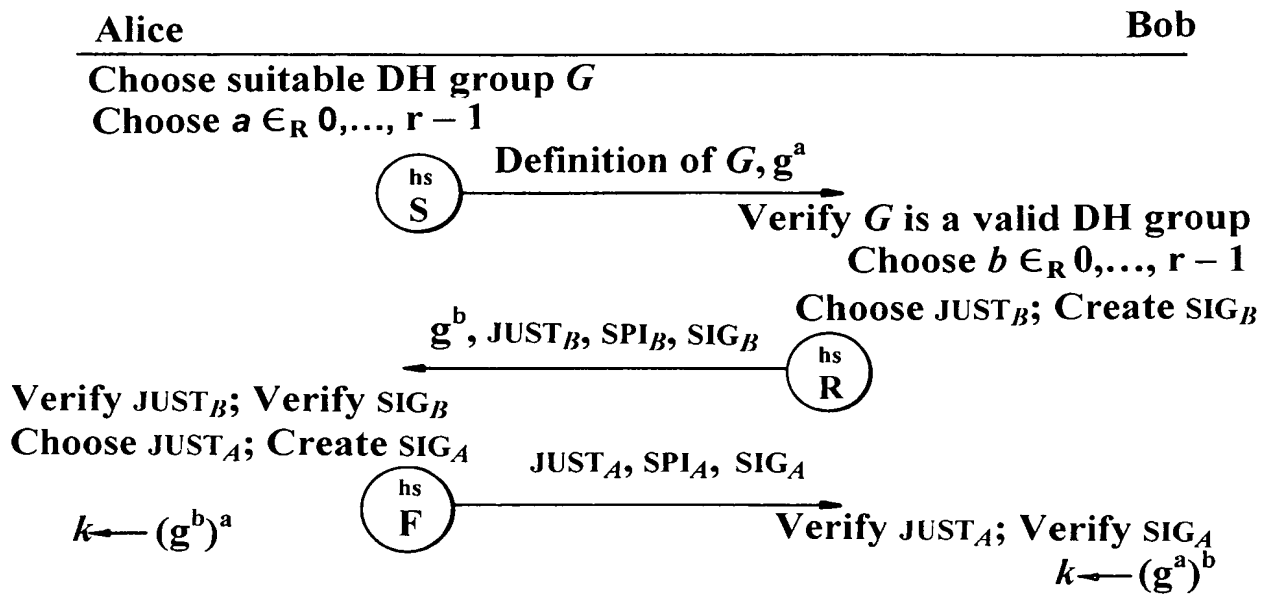


Fig. 6

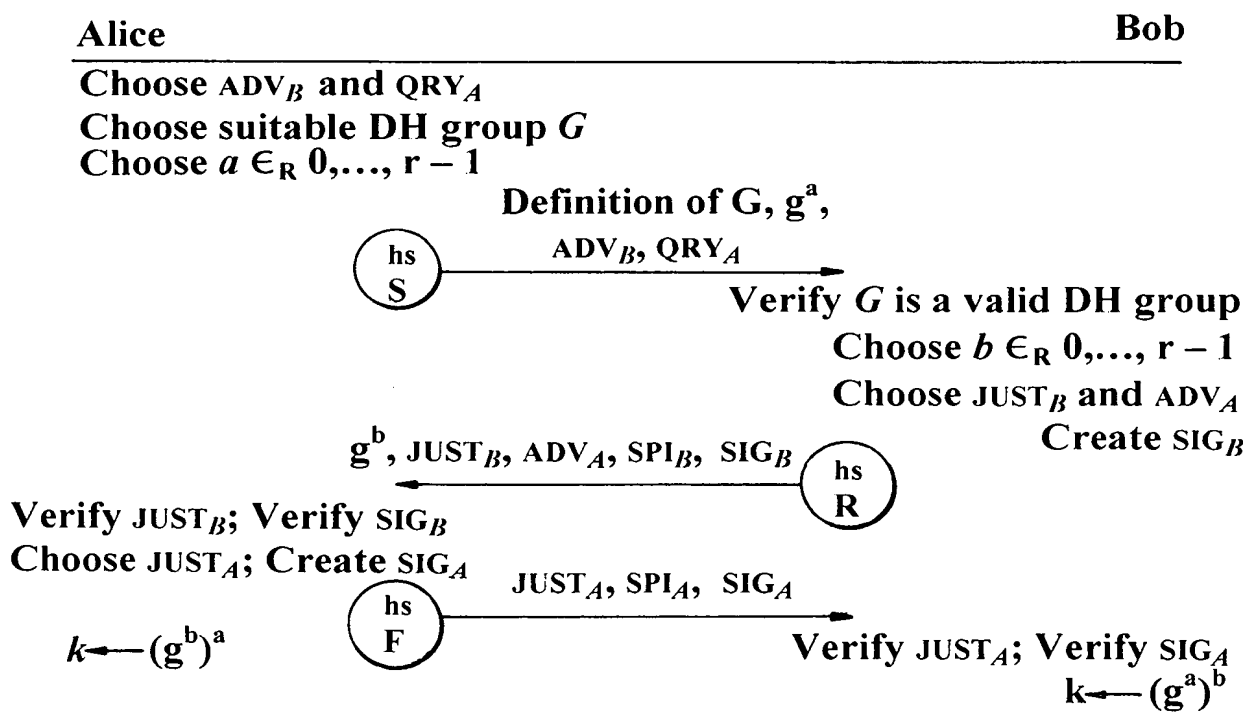


Fig. 7

Alice

Bob

Choose ADV_B and QRY_A
 Choose suitable DH group G
 Choose $a \in_R 0, \dots, r-1$
 Choose CS_L

Definition of $G, g^a, CS_L,$

hs
S

ADV_B, QRY_A

Verify G is a valid DH group

Choose $CS \in CS_L$

Choose $b \in_R 0, \dots, r-1$

Choose $JUST_B$ and ADV_A

Create SIG_B

$g^b, CS, JUST_B, ADV_A, SPI_B,$

SIG_B

hs
R

Verify $CS \in CS_L$

Verify $JUST_B$; Verify SIG_B

Choose $JUST_A$; Create SIG_A

$JUST_A, SPI_A, SIG_A$

hs
F

$k \leftarrow (g^b)^a$

Verify $JUST_A$; Verify SIG_A

$k \leftarrow (g^a)^b$

Fig. 8

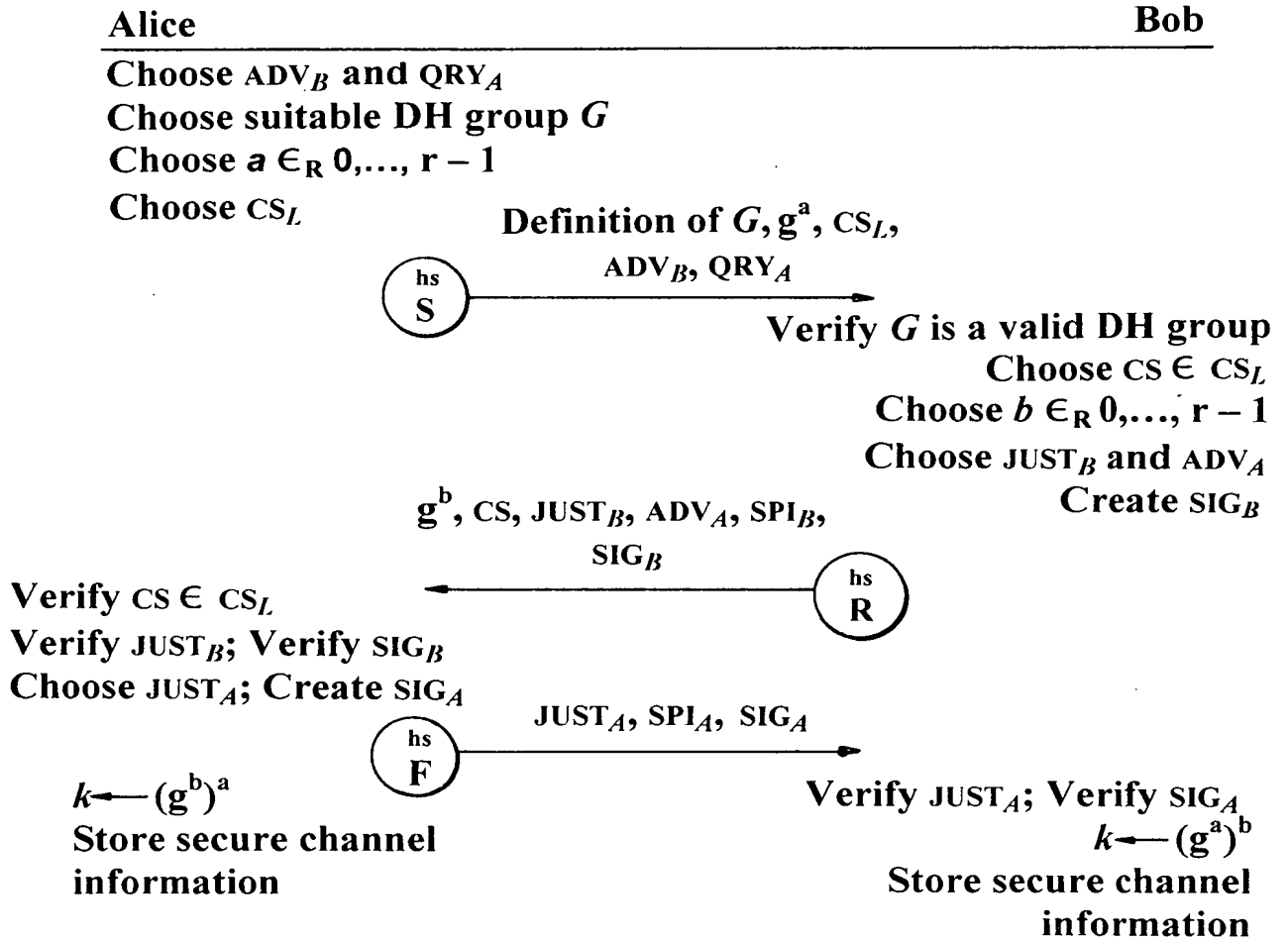


Fig. 9

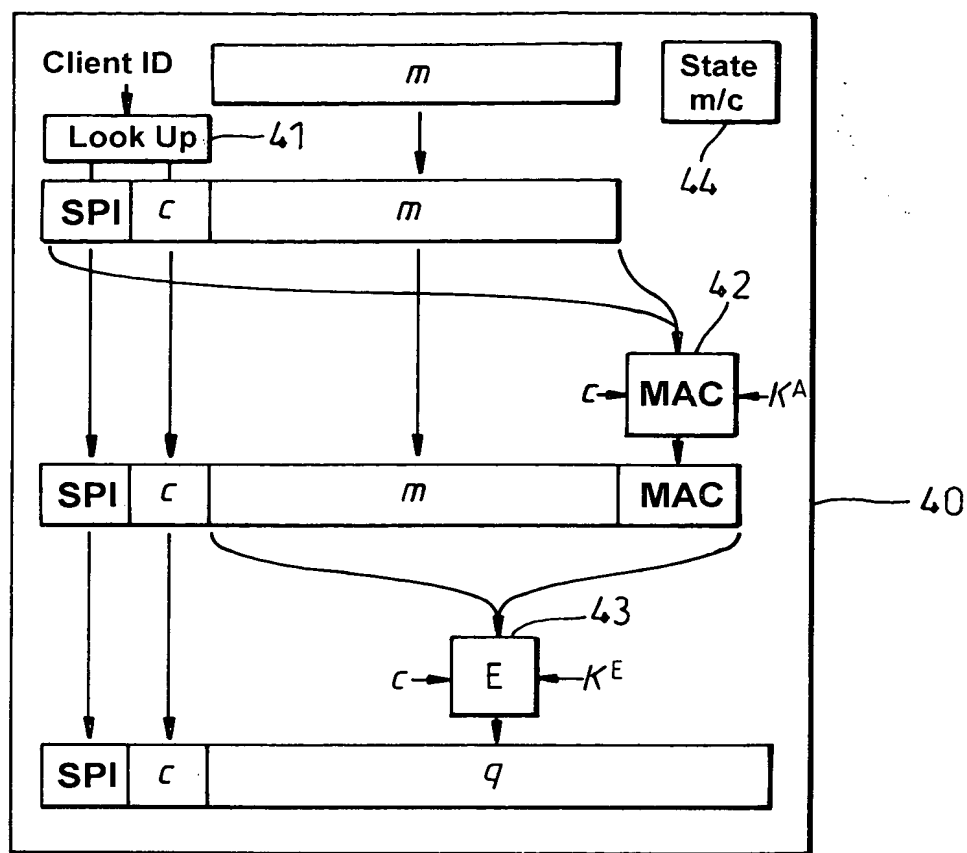


Fig. 10

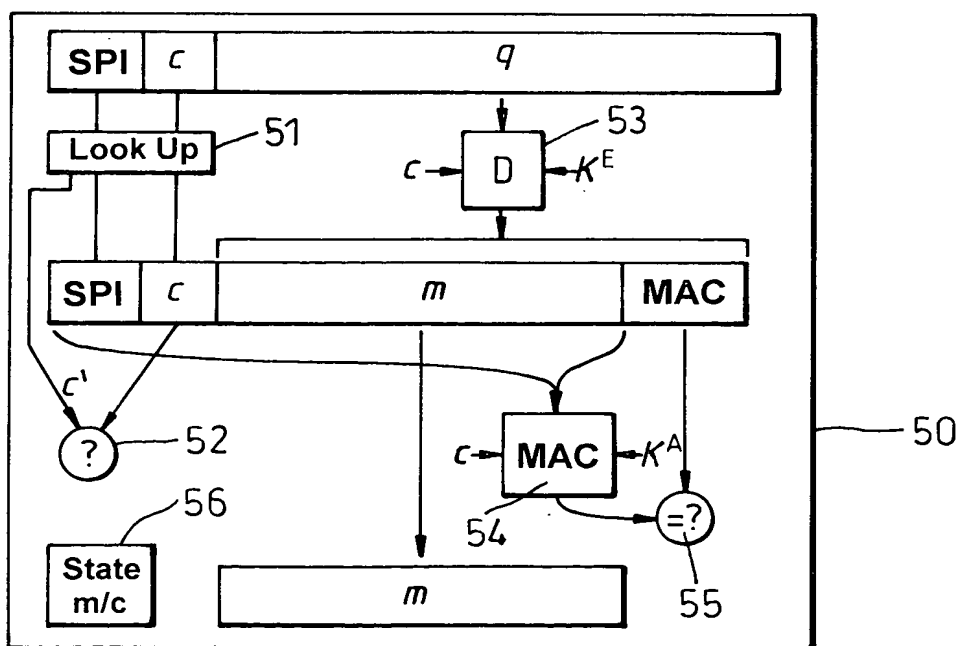


Fig. 11

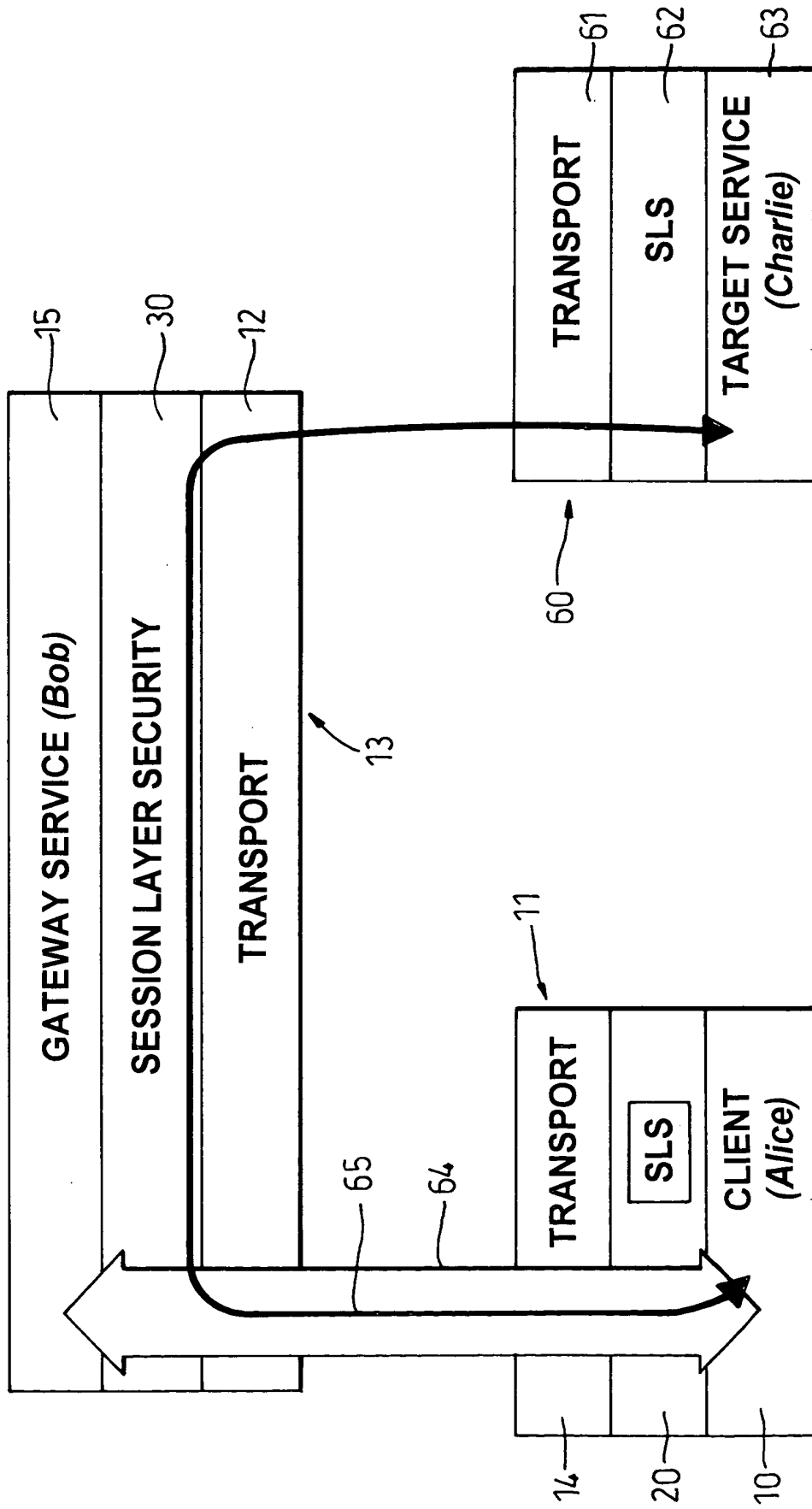


Fig. 12

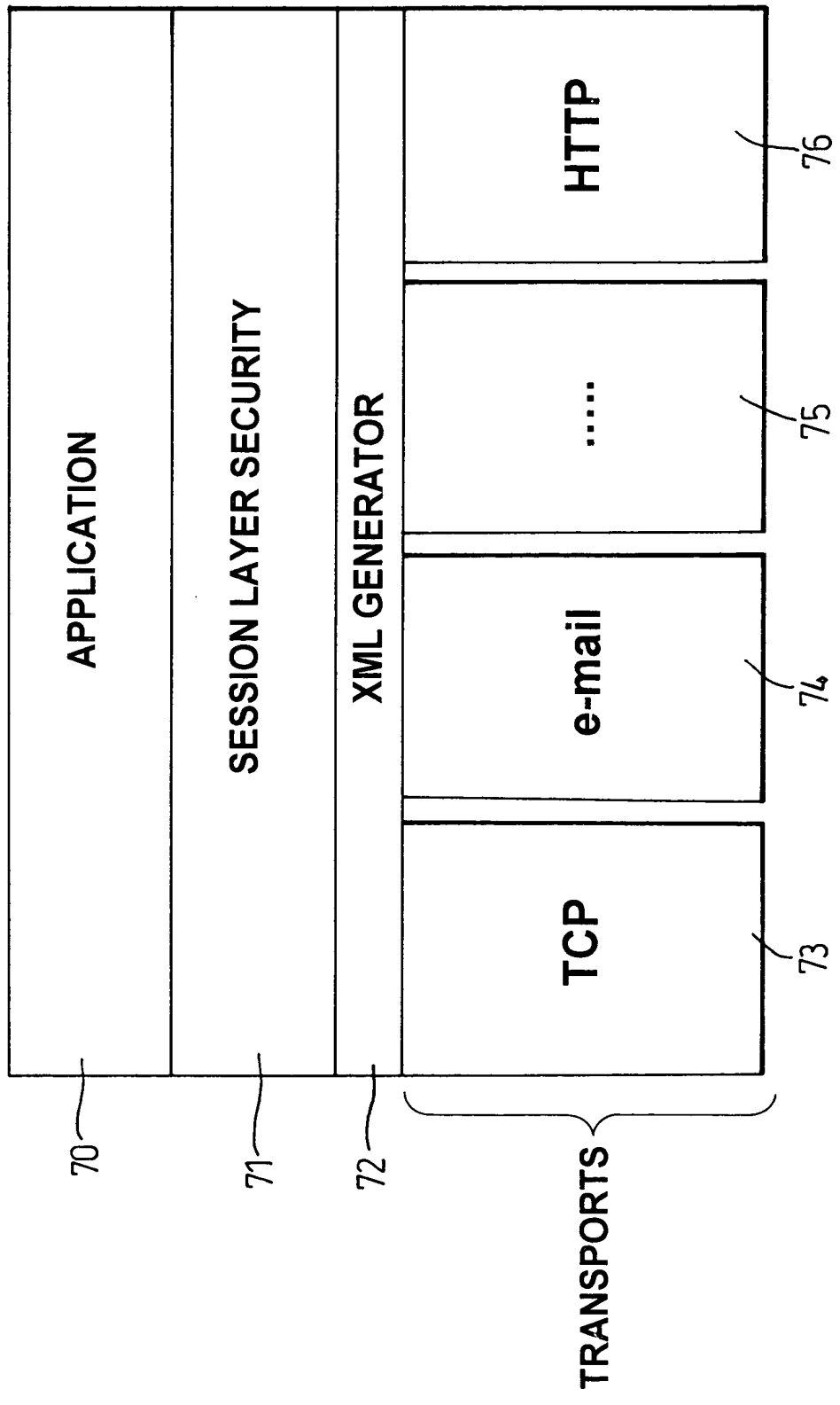


Fig. 13

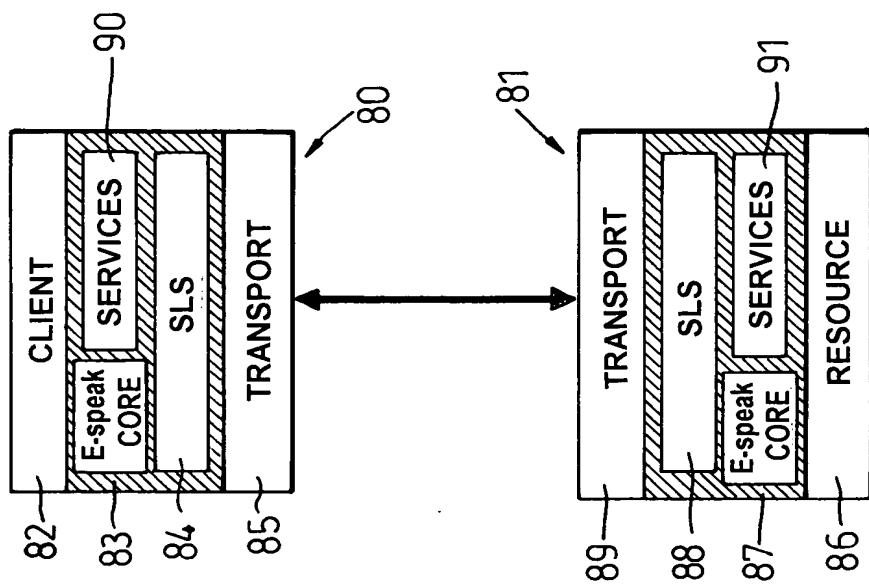


Fig. 14

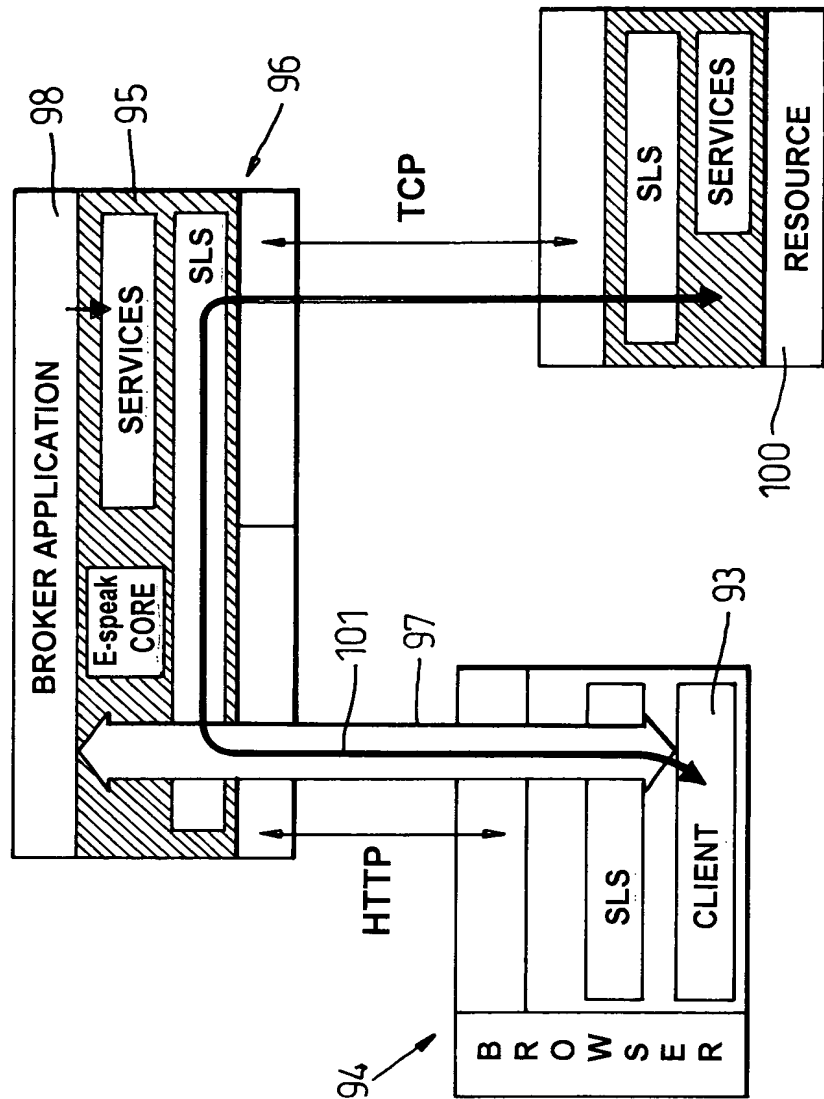


Fig. 15

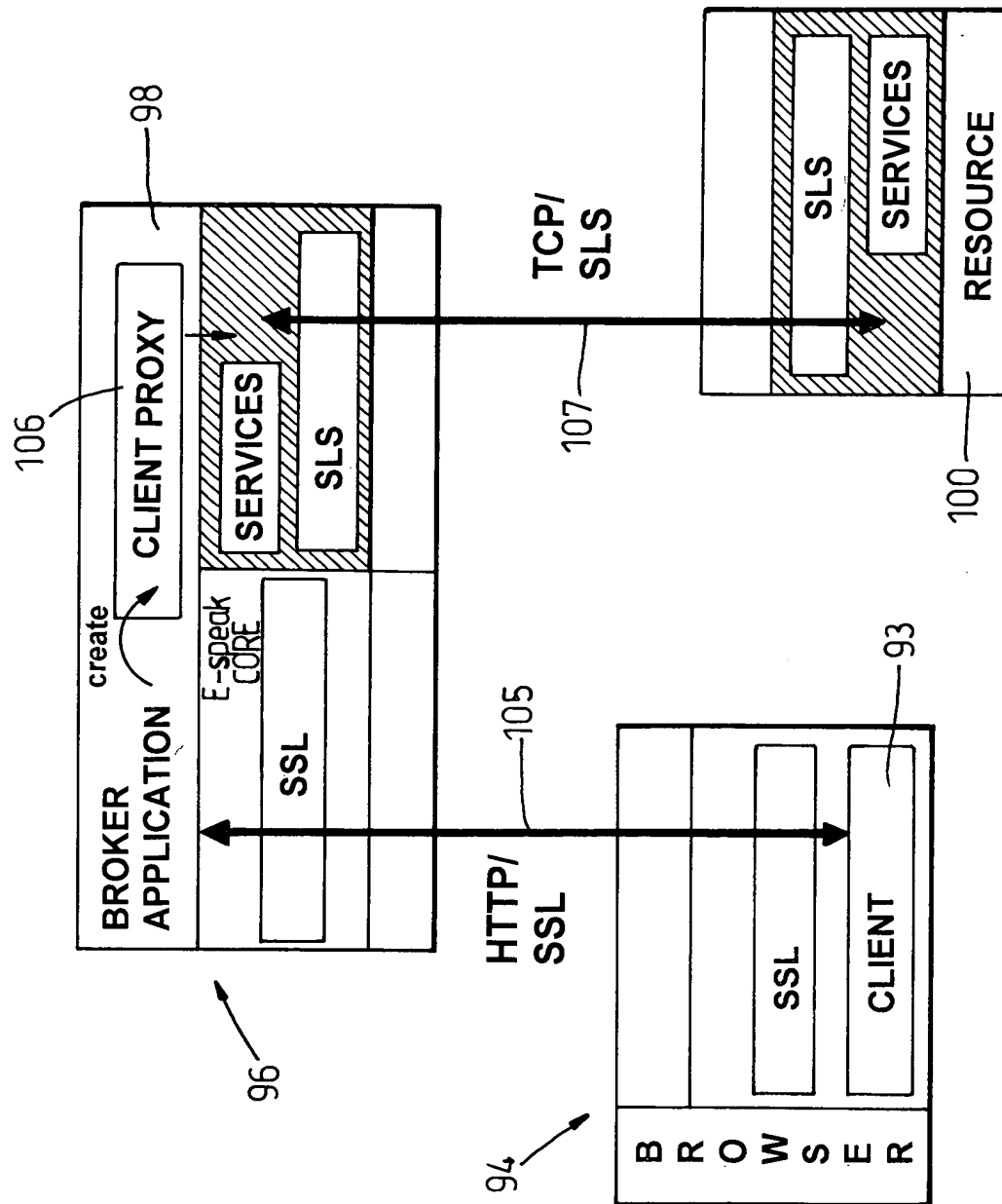


Fig. 16